Meeting the Technical, Staffing and Training Challenges of IPv6 Deployment

Dr. David Holder (Erion Ltd)
Mark McFadden
IPv6 Framework for European Governments – SMART 2016/0099
Workshop – Instituto Superior Técnico – Lisbon, Portugal
21st September 2018

Meeting the Technical, Staffing and Training Challenges of IPv6 Deployment

- Common Mistakes
- Meeting the Technical Challenges
- Meeting the Staffing Challenges
- Meeting the Training Challenges
- Resources Available to Member States
- Diverse Approaches for Diverse Public Administrations

Avoid the Most Common Mistake: IPv4 Thinking

- Do not understand the impact of legacy IPv4 thinking
- Legacy IPv4 thinking is an important IPv6 deployment project risk
- The extent of the differences between IPv4 and IPv6 is always underestimated
- Example: IPv6 Addresses (remember this is just *one* example out of many)
  - Assumption: The difference between IPv6 and IPv4 addresses is their length
  - Reality:
    - IPv6 addresses have different types from IPv4 (e.g. no broadcast)
    - IPv6 addresses have scope and lifetimes (IPv4 addresses do not)
    - It is normal for an interface to have multiple addresses and legal to have many
    - There are a large number of methods for assigning IPv6 addresses
    - Global public addresses are the norm
    - Addresses may change with time

Second Mistake: Underestimate the need for Education

- This is closely linked to the previous mistake, assuming that IPv6 is only IPv4 with longer addresses leads to underestimating the need for education

"In over twenty years of providing IPv6 training world-wide to organisations that include some of the world's leading technology companies we have found that they always underestimate the need for IPv6 training "

Dr. David Holder, Erion Ltd

"…as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know."

Donald Rumsfled, February 12, 2002

Beware too of IPv6 "unknown knowns" – things we know but refuse to accept

Meeting the Technical Challenges – First Steps

- Addressing the two most common mistakes in IPv6 deployments:
  - Ensure all staff are competent in IPv6
    - Education is crucial
  - Ensure that staff are working to an IPv6 agenda not an IPv4 agenda
    - Again, education is crucial

Meeting the Technical Challenges

- IPv6 is mainstream, it is common in many products, networks and services today
- Don’t under or over estimate the scale of the technical challenges
- Some technical aspects of IPv6 deployment are easy others are complex and require a good understanding of the technical details
- Pay particular attention to these areas:
  - Hardware and software (including locally developed apps and tools) readiness
    - Recent enterprise hardware and software is likely to be IPv6-ready. Legacy is likely to be problematic. Watch out for performance and resource issues
  - Your address schema and choice of address prefix/es
  - Security ideally you should have this in place already
  - Management (particularly DDI/IPAM and local tools)
  - Technical design decisions e.g. autoconfiguration methods, routing protocols, name resolver configuration and the use of transition mechanisms

Meeting the Technical Challenges - Hardware

- Most modern enterprise hardware is “IPv6-ready”
- Your existing infrastructure’s support for IPv6 will vary
  - Very old equipment may not support IPv6 at all
    - This equipment will continue to work in a dual-stack environment using IPv4
    - If IPv6 support is required for IPv6 deployment then it will may need to be replaced or supplemented
  - More recent equipment may support different sets of RFC depending on age
    - You may need to carry out an IPv6 support audit
      - This will depend on the functionality required and the equipment involved
  - Hardware resource limitations may be a problem
    - Requirements for just IPv4 are different from requirements for IPv4 *and* IPv6
    - Memory capacity may be exceeded
  - Legacy equipment may support IPv4 in hardware and IPv6 in software

Meeting the Technical Challenges – Software

- Most modern networked software supports IPv6
- Despite this some software does not support IPv6:
  - There remain commercial products that do not support IPv6
  - Legacy versions of software
  - Internal systems:
    - Line of business applications
    - Web applications
    - System and network management tools
- IPv4 applications will continue to work in dual stack environments
- Legacy IPv4 applications can often be accessed over IPv6 using proxies or translation – they appear to be IPv6 enabled even if they are not
- Internally developed software may need to rewritten
- Software providers may need to IPv6 enable their products

Meeting the Technical Challenges – Address Schema

- Designing the address schema requires a detailed knowledge of IPv6 addressing
  - Choice of structure: topology, function or a mixture of the two
  - Integration with existing IPv4 infrastructure
  - Leverage of large address space
  - Subnet structure
  - Choice of interface identifiers (IIDs)
  - Relationship to name resolution
  - Allocation policy
  - Interlink allocations
  - Node assignments
  - Security considerations
  - Address management

Meeting the Technical Challenges – Address Prefix

- Two key decisions: the source of prefix and the type of prefix
- Prefix type
  - Provider Aggregatable (PA) space
    - Space assigned to an LIR that is then assigned to End Users and/or sub LIRs
    - End Users using PA space that move provider will be allocated a different prefix and will therefore be forced to renumber their networks
  - Provider Independent (PI) space
    - Space assigned to End Users that is independent of the provider/s they use
    - PI space must be advertised by the End User or by their upstream provider
- Prefix source
  - PA and/or PI space can be obtained from an LIR
  - Only an LIR can obtain PA space from a RIR (e.g. RIPE)
  - An LIR can also obtain PI space from a RIR (e.g. RIPE)

Meeting the Technical Challenges – IPv6 Security

- All modern networks are IPv6 capable (and enabled) by default
- IPv6 security should already be a part of your security policy and operations
- IPv6 security is different from IPv4 security and includes many new challenges
- There are implications for all parts of your security infrastructure:
  - Security personnel (training and experience with IPv6)
  - Edge security (firewalls, NIDS etc)
  - Internal security
  - LAN security
  - First-hop security
  - Node security (host, server and network devices)
  - Logging, monitoring, forensics and auditing

Meeting the Technical Challenges - Management

- A key step in deploying IPv6 is upgrading systems and network management tools to support IPv6
- This includes both commercial, open-source and internally developed tools
- Must provide equivalent support for IPv6 as for IPv4
- Must be able to handle differences in IPv6
  - Longer addresses
  - Multiple addresses per node
  - Addresses that change with time
  - Special address formats (URL, URIs, UNCs, Email addresses etc)
- For example, if you are collecting flow data using Netflow or IPFIX then you will need to ensure that you are using at least Netflow v9 and that your exporters, collectors and analysis tools support IPv6

Meeting the Technical Challenges – Design Decisions

- Autoconfiguration methods
- Routing protocols
- Name resolver configuration
- Name resolution
- Choice and use of transition mechanisms
- Platform configuration:
  - Routers and network infrastructure
  - Firewalls, IDS, NIDS and security infrastructure
  - Servers
  - Workstations and laptops
  - Mobile devices
  - Applications
  - Internet of Everything (IoE)

Meeting the Staffing Challenges

- Staff need to be IPv6 aware
- Staff need to be retrained to have an IPv6 worldview (and see IPv4 as legacy)
- Staff who are key to the IPv6 deployment project need to be proficient in IPv6
- Staff who are responsible for network design, planning, deployment, operation, security, support and software development need to be at least as proficient in IPv6 as they are in IPv4
- Network professionals with experience of deploying IPv6 are rare

- Three solutions:
  - Hire people with the necessary IPv6 skills (only useful with new staff)
  - Train existing staff (see later)
  - Use contract resources or consultancy services

Meeting the Training Challenges - Background

- IPv6 education is pivotal to the success of an IPv6 deployment
- All reports of IPv6 deployments attest to the importance of IPv6 training
- Education is essential for architects, administrators, developers and support staff
- You need to:
  - Understand the need for training
  - Identify the groups of staff who will require training
  - Prioritise the training of key players in the IPv6 deployment project
  - Determine when the training will be required
  - Determine how the different groups should be trained
- Beware of:
  - Out-of-date material and guidance (this is common)
  - Appreciate that unlearning legacy IPv4 habits is non-trivial

Meeting the Training Challenges - Approaches

- Three main categories of training approaches:
- No training
  - Hire or contract staff with the necessary skills and experience
- Awareness
  - For staff with limited networking exposure you can provide self-learning materials, documentation, guides, whitepapers, web-sites, videos, Computer based training (CBT) and short introductory sessions
- Formal Training
  - Staff directly involved in network administration, network security, system administration, network support and software development are likely to require targeted formal training. Usually this will be instructor led. We have found that *all* organisations underestimate the IPv6 training that they require.

Embed IPv6 into all network related training and induction materials

Meeting the Training Challenge – Examples I

Training Area	Target Audience	Days
IPv6 for Helpdesk Staff	Support and Helpdesk Staff	1
IPv6 Introduction/Overview	IT Managers/Project Managers	1
IPv6 Awareness	General ICT Staff	1
Implementing IPv6	Staff involved in design and deployment of IPv6	4
IPv6 Security	Staff involved in network security	4
Implementing IPv6 on Windows	Specialists in Windows	4
Implementing IPv6 on Linux	Specialists in Linux	4
Implementing IPv6 on Cisco IOS	Specialists in Cisco	4

Meeting the Training Challenge – Examples II

Training Area	Target Audience	Days
Implementing IPv6 on Juniper	Specialists in Juniper	4
IPv6 Forensics	Staff involved in network security, incident response and NOC staff	5
IPv6 for Software Developers	Developers writing networked applications	4
Implementing and Securing IPv6	For system administrators and security personnel	5
Management Overview IPv6	Senior managers	0.5

Meeting the Training Challenge – Planning

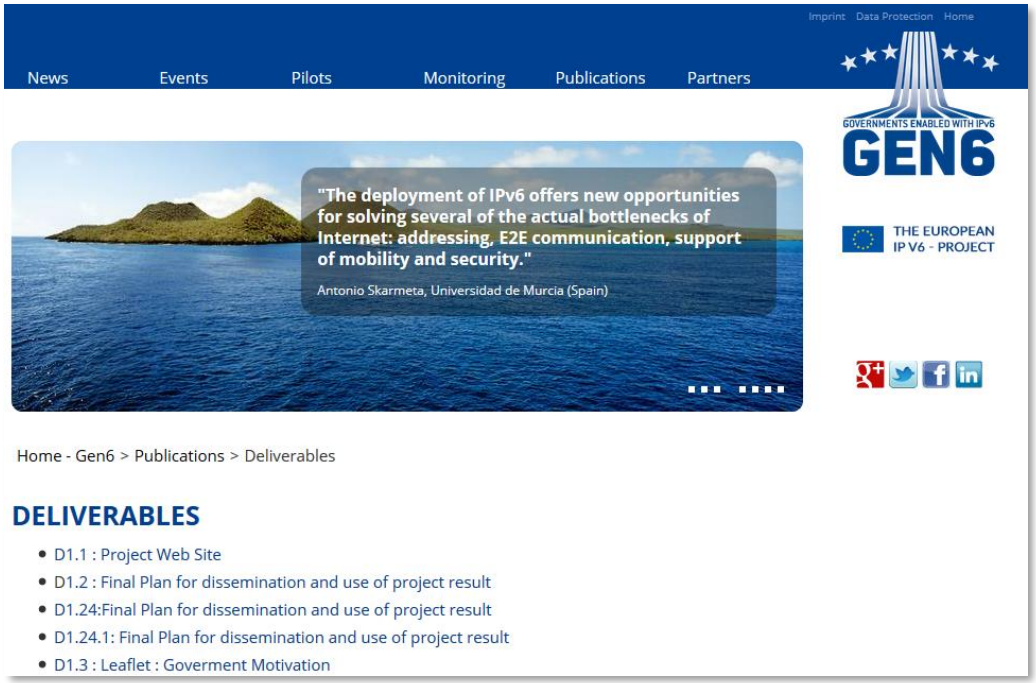
- You should create an IPv6 Awareness and Education Programme plan
- Your IPv6 Awareness and Education Programme plan should:
  - Identify who needs training
  - Identify key project players who require expedited training
  - Determine when they should be trained
  - Specify the type of training most appropriate
  - Specify specific training courses or resources

IPv6 Resources Available to Member States

- GEN6 part of an ISA2 project that piloted IPv6 deployments in member states
  - Includes training/education/case study materials to help member states
  - http://www.gen6-project.eu/
- IPv6 Framework for European Governments – SMART 2016/0099 (this project)
  - Provides documents to assist in IPv6 technology transfer and deployment
    - Synthesis of the status of IPv6 in European member states
    - Guidelines and process: IPv6 for public administrations in Europe
    - Technical profiles: IPv6 for public administrations in Europe
    - IPv6 address acquisition in Europe
    - Interim report on this project
    - Future resources to be added include materials from this workshop
  - http://ipv6gov.eu/

Resources Context – ISA2 Pilot Project

- A previous ISA2 project piloted IPv6 deployments in a selection of member states
- Part of that project – called GEN6 – was building training / education / case study materials that would help Member States as they considered IPv6 deployment
- The GEN6 materials are online and available at:
  - http://www.gen6-project.eu/



Resource Materials from this Project

- This is an implementation project focused on the technology transfer that:
  - Helps provide documentation for starting an IPv6 transition
  - Explains mechanisms for acquiring IPv6 addressing
  - Describes implementation plans that vary based on the size of the public administration
  - Provides the basics of building IPv6 addressing plans for a new or existing network
  - Describes approaches to IPv6 deployment planning

- These materials are available from the project website at:
  - http://ipv6gov.eu/

Synthesis of the Status of IPv6 in Europe MS

- A comprehensive examination of IPv6 deployment in public administrations
- Based on research conducted in October 2017 to March 2018
- Comprehensive: attempts were made to interview every European MS
- Data provided includes projects underway, key stakeholders and how the MS is doing regarding IPv6 deployment
- Provides key observations about trends in IPv6 deployment in public administrations
- Helps identify those countries that have had success in deployment
  - With the possibility of learning how to overcome barriers to deployment

- These materials are available from the project website at:
  - http://ipv6gov.eu/wp-content/uploads/2018/05/IDATE-EC-IPv6-Country-Profiles.pdf
  - http://ipv6gov.eu/wp-content/uploads/2018/05/IDATE-EC-IPv6-Country-Profiles-Executive-Summary.pdf

IPv6 Guidelines and Process

- Guidelines and Process: IPv6 for Public Administrations in Europe
  - IP Addressing Basics
  - Host Addressing Assignment
  - Why is IPv6 Different for Public Administrations
  - Planning the Public Administration Deployment
  - IPv6 Subnetting
  - Getting IPv6 Addresses
  - IPv6 Address Maintenance
  - RIPE Requirements for IPv6 Compliance (RIPE-554)
  - Special Use IPv6 Addresses

  - http://ipv6gov.eu/wp-content/uploads/2018/05/Plum-EC-IPv6-Guidelines-in-public-administrations.pdf

IPv6 Technical Profiles

- Technical Profiles: IPv6 for Public Administrations in Europe
  - Planning for IPv6 in Public Administrations
  - Transition Approaches and Technologies
  - Existing Profiles from other Countries
  - Profiles for IPv6 Hardware
    - Fundamentals
    - Edge Systems and Mobile Devices
    - Routers
    - Infrastructure Networking
    - Management Devices
  - http://ipv6gov.eu/wp-content/uploads/2018/05/Plum-EC-IPv6-Technical-Profiles.pdf

IPv6 Address Acquisition in Europe

- A short guide for public administrations on how to obtain IPv6 addresses
- Covers types of addresses to be acquired
- Then examines
  - Getting IP addresses from upstream providers including national services
  - Becoming an LIR in the RIPE region in Europe
    - Step-by-step description of the process
    - Likely results
    - Examination of the growth of LIRs in the RIPE region
  - Intended as a short guide to IPv6 address acquisition
    - Non-technical approach to the subject matter

Summary of the First Part of this Project

- An interim report on the first two phases of this project and a description of what is yet to come
- Written at a very high level
  - Non – technical
- Fulfills a requirement of the project, but provides the non-technical

Future IPv6 Resources from this Project

- A meeting report from the first workshop is available on the project website
- Training materials for future workshops will be made available
- In the future, as other materials are developed
  - They will be made public on the project website
  - Along with the descriptions of the content and purpose of those new materials
- Final project report and presentation will be made public on the project website
- In addition to this project, there are many other resources for IPv6 deployment
  - Very few are targeted specifically at public administrations
  - Few deal with the specific barriers that confront public administrations
  - Many are built to motivate private sector transition

Diverse Approaches for Diverse Public Administrations

- There is no one solution that is appropriate for all public administrations
- IPv6 deployment can be undertaken in many different ways
  - IPv6 itself has been designed to provide great flexibility in how it is deployed
    - You can start in different places; core, edge, node, application, translation…
    - You can enable parts of your infrastructure at different times
    - You have many design options for configuration and management
  - This flexibility can be leveraged to match the diverse range of scenarios in public administrations
  - Flexibility can be both an advantage and a challenge – many choices to make
  - If you look at case studies from other member states you will notice that there are many things that they have done differently

Case Studies in Successful Deployments

- Commercial
  - Facebook – additional information
  - Microsoft

Case Study: Facebook Technical Challenges

- Everyone is excepted to use IPv6 as the default and in some cases the only means to carry out their work. All work must be IPv6 ready.
  - Servers can only be managed over IPv6
- A number of technical challenges were overcome:
  - Dual stack deployment would have exceeded resources so a phased moved to IPv6-only was adopted
  - Some equipment is IPv4-only, for example, remote console servers. This equipment is gradually being removed during equipment refresh cycles.
  - Facebook's environment hit performance problems with Linux cached routing entries that are used for recording Path MTU (PMTU). Millions of entries were being created as Linux used a cached route for each and every path. Facebook developed a change to the Linux kernel that solved this.
  - All Facebook's management tools had to be updated to support IPv6 before the deployment began
- Guest WiFi is IPv6-only

Case Study: Microsoft

- Company
  - 113,000+ employees (220,000 end users including external ones)
  - Four regions with smaller campuses and tail sites (800 locations)
  - 1900 Line of business applications
  - 1.2 million devices hitting the network daily
- History
  - 2001 – Microsoft Research began with ISATAP deployment
  - 2006 – Native IPv6 became more widely deployed
  - 2011 – IPv6 became strategic goal
    - Dual stack roll-out
    - Bought Nortel address space & internal public space freed for cloud services
  - 2016 – Retrofit native IPv6 to all corporate networks
    - Still have many networks that are IPv4-only

Case Study: Microsoft

- Key Stakeholders
  - Enterprise commitment to IPv6 at all levels – strategic goal since 2011
- Drivers to Adopt IPv6
  - Shortage of public IPv4 address space
    - For cloud (Azure/Office365) and other services
    - Exhausted RFC1918 space
    - Unable to obtain additional large continuous IPv4 blocks
- Current goal is IPv6-only
  - IPv6-only is strategic goal as IPv4 costs money
  - MS has over 89 apps in the Apple AppStore (must be IPv6-only since 2015)
  - Widely deployed IoT
  - Overlapping RFC1918 address space
  - The operational complexity of dual stack

Case Study: Microsoft Technical Challenges I

- Wireless guest IPv6-only
  - Aim was to use a relatively easy environment to test IPv6-only
  - Proved to be less easy than expected:
    - Need to deploy NAT64/DNS64
    - Breaks guests VPN clients that do not support IPv6 or NAT traversal
    - Had to pause this project – will be returned to in next 12 months
- IPv6-only Wireless SSID for Product Groups (App testing)
  - Production for IPv6-only apps
  - Test requirements for Apple AppStore and US Federal Government
  - Uses NAT64/DNS64
  - Requires RDNSS for Android (no DHCPv6 support) – required updates
  - Widely deployed and deployment continuing

Case Study: Microsoft Technical Challenges II

- Remote Access VPN
  - Over 50,000 VPN users
  - Dual stack on the inside, IPv4 at the edge
  - Driver for IPv6 is that networks with IPv4 as a service (IPv4AAS) can break VPNs (e.g. Comcast, Charter and Free)
    - Need VPN to be dual stack to allow IPv6 to be used in IPv4AAS environments
  - VPNs also are a big consumer of IPv4 address space
    - IPv6 will free some of this up
  - They are also carrying out a proof of concept of IPv6-only on the inside

Case Study: Microsoft Technical Challenges III

- IPv6-only technical challenges:
  - Some products that support dual-stack do not support IPv6-only
  - For example
    - IPv6-only VPN profiles were not supported on some products
    - Wireless RADIUS authentication over IPv6 was not supported on some products
    - WLAN management over IPv6 – one vendor does not support automatically discovering APs over IPv6 – firmware update will fix this…
    - Cloud services are often not IPv6 ready – e.g. security features/products
    - Network and infrastructure management, suppliers say IPv6-only is supported, often it is not
    - Docking station lock-up – it did not like router advertisements

Case Study: Microsoft – Key Lessons

- Perseverance is necessary – it will take a long time
- Communication is essential
  - IPv6 newsletter
  - IPv6 position paper
  - IPv6 strategy
  - IPv6 awards
- Only IPv6-only makes sense in the long-term
- Microsoft and IPv6
  - 85% of global laptops are Windows
  - Hundreds of millions of devices are Windows based
  - How long will Microsoft continue to support IPv4?

Questions and Discussion